PROTECTING WEB SITES

حماية مواقع الإنترنت

الدرس الأول

الدرس الأول

- أهداف الدرس :
  - أن يعرف الطالب أضرار اختراق مواقع الويب .
  - أن يعرف الطالب مفهوم اختراق مواقع الويب .
  - أن يتناقش الطالب مع زملائه في طرق حماية مواقع الويب علي مستوي الخادم server .

  - أن يتناقش الطالب مع زملائه حول طرق حماية مواقع الويب علي مستوي مطوري الخادم حيث :
  - يقسم المعلم الفصل إلي عدة مجموعات .
  - يطلب من جميع المجموعات التوصل لطرق حماية مواقع الويب علي مستوي مطوري الخادم .
  - يتناقش الطلاب مع بعضهم البعض داخل المجموعة الواحدة .
  - يكافئ المعلم أفضل مجموعة ويعرض نتاج نقاشها علي باقي المجموعات للاستفادة منها .
  - أن يناقش الطالب زملائه في بعض الإرشادات الخاصة بالحفاظ علي مواقع الويب من الاختراق .
  - أن يؤمن الطالب مواقع الويب من الاختراق بإتباع بعض الإرشادات الخاصة بالحفاظ علي مواقع الويب من الاختراق .

أهلا بك عزيزي الطالب في الدرس الأول الذي يتضمن الموضوعات التالية :

- ما النتائج المترتبة علي اختراق مواقع الويب ؟
- مفهوم الاختراق .
- طرق حماية مواقع الويب .
- بعض إرشادات تأمين مواقع الويب .

شرح موضوعات الدرس :

- **أولاً : ما النتائج المترتبة علي اختراق موقع ويب ؟**
  - يعتبر تأمين مواقع الويب ضرورة تفرض نفسها وذلك للحد من اختراقها ، والذي يمكن أن ينتج عنه الآتي :
  - فقد البيانات والتي قد تكون هامه وتؤدي إلي خسائر مالية لبعض المؤسسات .
  - سرقه بيانات هامة من الموقع .
  - الحصول علي بيانات مؤسسية أو شخصية وما لهذا من أضرار بالغة بعد ذلك .
  - عرض محتوي آخر غير ملائم قد يحتوي علي توجيهات سياسية أو دينية أو أخلاقية غير مرغوبة .
  - تشويه صورة المؤسسة أو الشخص صاحب الموقع بشكل عام ، وبالتالي يؤدي إلي فقدان ثقة المستخدمين والزائرين في الموقع .

ثانياً : مفهوم الإختراق :

- يعبر عنه عادةً بـ web site hacking حيث يمكن للمخترق من الحصول علي صلاحية التحكم في إدارة الموقع أو التعامل مع بيانات الموقع بأي صورة (عرض – حذف – تعديل - ..... الخ) من خلال استغلال ثغرة أمنية أو برمجية ضعيفة .

نشاط (1) :

- اسم النشاط : ما مفهوم اختراق مواقع الويب وما **النتائج المترتبة علي الاختراق ؟**
- هدف النشاط : أن يساعد الطلاب بعضهم البعض في معرفة مفهوم الاختراق وفي التوصل إلي النتائج المترتبة علي الاختراق .

ثالثاً : طرق حماية مواقع الويب :

- تنقسم طرق حماية مواقع الويب إلي قسمين وهما :-
  - حماية علي مستوي الخادم (server) أو الخادم المستضيف للموقع(web site Hosting)
  - وتكون الحماية هنا مسئولية الخادم أو الجهة المستضيفة للموقع والتي يجب أن تقوم بإعداد خيارات الأمان بشكل صحيح .
  - حماية علي مستوي مطوري الموقع.

وتكون الحماية هنا مسئولية مطوري الموقع والمسئولين عن إدارته مثل :

- التحقق من المدخلات قبل تخزينها في قاعدة البيانات.
- تشفير كلمات المرور .
- إدارة مجلدات الموقع الهامة بكلمات سر قوية .
- تحديد صلاحيات للمستخدمين بشكل صحيح .

نشاط (2) :

- اسم النشاط : طرق حماية مواقع الويب التي يجب إتباعها للمحافظة علي مواقع الويب من الاختراق .

- هدف النشاط : أن يشارك الطالب زملائه في العمل الجماعي داخل المجموعة الواحدة ويتناقش معهم حول طرق حماية مواقع الويب من الاختراق .

رابعاً : بعض الإرشادات للحفاظ علي الموقع مؤمناً :

تحديث البرامج KEEPING SOFTWARE UP-TO-DATE

- يجب التأكد من الحصول علي التحديثات الخاصة بالبرامج المستخدمة في إدارة وتصميم الموقع سواء كانت برامج نظم تشغيل الخادم أو أي برامج أخري تعمل علي الموقع .

التعامل مع رسائل الخطأ ERROR MESSAGES

- من الضروري التعرف علي كافة الأخطاء المحتملة أثناء تصميم الموقع ، ولكن عند نشر الموقع يجب الحرص علي إخفاء الأخطاء ، حيث أن هذه الأخطاء تجعل الموقع ضعيف وأكثر عرضة للاختراق.

- ويتم التعامل مع الأخطاء عن طريق توقع الخطأ والتعامل معه برمجياً مثل جملة Try….catch من خلال رسائل معدة بعناية ولا توحي للمستخدم بأي معلومات قد تستخدم في الاختراق مثلاً عند وجود خطأ في كلمة السر يمكن إعطاء رسالة " اسم المستخدم أو كلمة السر غير صحيحة " .

التحقق من صحة البيانات المدخلة من المستخدم
INPUT DATA VALIDATION

- عدم التحقق من البيانات المدخلة يعطي فرصة لذوي النوايا السيئة باختراق الموقع بإدخال مدخلات معينة تسبب في الاختراق ومن أهم قواعد الحماية من الاختراق مثلاً التحقق من أن الحقل غير فارغ ويحتوي علي قيم معينة لا تزيد عن عدد محدد من الأحرف وذلك باستخدام جملة If .

كلمات المرور PASSWORDS

- يجب أن تكون معقدة نوعاً ما حتى يصعب علي المخترق اكتشافها وخاصةً كلمة مرور الخادم server وكلمة المرور admin الخاصة بالموقع وكلمات مرور قاعدة البيانات .

تجنب حقن جمل SQL (SQL INJECTION)

- حيث يقوم المخترق بإدخال معامل خاص في جمله (SQL) بدلاً من إدخال اسم المستخدم بهدف إحداث تعديلات غير مرغوبة بجداول قاعدة البيانات .

تجنب كتابة كود عبر الموقع XSS(CROSSE SITE SCRIPTING)

- يقصد بها حقن أو إدراج كود في صفحات موقع والخطورة تكمن في قبول هذا الكود لعدم وجود برمجة تحقق من المدخلات ، ويمكن تجنب ذلك باستخدام أسلوب البرمجة المناسب مثل عدم السماح مثلا بأي كود script في حقل التعليقات .

رفع الملفات FILE UPLOADS

- إن السماح برفع ملفات إلي موقعك يحتوي علي مخاطرة كبيره يجب الاحتراس منها بالاحتياطات البرمجية اللازمة ، ويتم علاج هذا الاحتمال بعمل اختبار للملف المفترض فإذا كان ملف صورة مثلاً توفر لغة php العديد من أساليب البرمجة للتأكد من هوية الملف.

استخدام تطبيقات تأمين مواقع الويب WEBSITE SECURITY TOOLS

- بعد الانتهاء من تصميم الموقع يجب اختبار أمان الموقع عن طريق استخدام تطبيقات أمان الموقع ويوجد العديد من هذه التطبيقات منها ما هو مجاني أو مفتوح المصدر .
- أمثله من هذه التطبيقات :
- Open VAS ويعتبر من أكثر التطبيقات مفتوحة المصدر استخداماً لاختبار أمان الموقع .
- Net sparker وهو جيد لاختبار SQL Injection and XSS

نشاط (3) :

- اسم النشاط : " طرق اختراق مواقع الويب التي يجب تجنبها .

- هدف النشاط :أن يساعد الطالب المتفوق زملائه في الفصل للتعرف علي طرق اختراق مواقع الويب التي يجب تجنبها .

المطلوب :

- إكمال العبارات بالمفهوم العلمي المناسب مما يلي :
- SSL(Secure Sockets Layer) – Open VAS_ SQL Injection – XSS(Cross site scripting) – MD5.
- .....يعتبر من أكثر التطبيقات مفتوحة المصدر استخداماً لاختبار أمان الموقع
- ..... يمكن أن يتم عن طريق إدخال المخترق لجملة SQL بدلاً من إدخال اسم المستخدم بهدف إحداث تعديلات غير مرغوبة بالجداول .
- ..... هو بروتوكول لتأكيد التعامل الامن بين خادم الويب Web Server ومستعرض الانترنت Web Browser عن طريق توسيط طرف ثالث يسمي Certificate Authority .
- ..... أحد أساليب تشفير البيانات المتاحة في لغة PHP .